T.C.
İSTANBUL TEKNİK ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

AĞ GÜVENLİĞİ
Prof. Dr. Bülent ÖRENCİK

Matematiksel Kriptoanaliz

Müh. Ferhat Karakoç
504051509

İçindekiler

Matematiksel Kriptoanaliz 1
İçindekiler 2
1 GİRİŞ 3
2 KRİPTOANALİZ 3
2.1 Tanım 3
2.2 Kriptoanaliz Yaklaşım Tipleri 3
2.2.1 Elektronik Kriptoanaliz 3
2.2.2 Matematiksel Kriptoanaliz 4
2.2.3 İki Yaklaşımın Karşılaştırılması 4
3 MATEMATİKSEL KRİPTOANALİZ 4
3.1 Tanım 4
3.2 Yöntemler 4
4 SP NETWORK 4
5 LİNEER KRİPTOANALİZ 7
5.1 S-box'ların Lineerleştirilmesi 9
5.2 SP Ağının Lineerleştirilmesi 11
6 SONUÇ 15
7 KAYNAKLAR 16

1 GİRİŞ

Bilgi güvenliği, geçmişten günümüze kadar önemli bir kavram olmuştur. Bu güvenliğin sağlanması için şifreleme sistemleri geliştirilmiş ve bu sistemlerin güvenilirlik bakımından sağlamlığının analizi için de kriptoanaliz gelişmiştir. Özellikle son bir asırdır şifreleme sistemlerinin karmaşıklaşmasından dolayı matematiğin kriptoanalizde önemi artmıştır.

Bu çalışmanın başlığı her ne kadar "Matematiksel Kriptoanaliz" olsa da içeriğini matematiksel kriptoanaliz yöntemlerinden bir tanesi olan lineer kriptoanaliz oluşturmaktadır.

2 KRİPTOANALİZ

2.1 Tanım

Kriptoanaliz, bir kripto sisteminin sağlamlığının analizi şeklinde tanımlanabilir. Burada sağlamlık, sistemin kırılamaması anlamına geliyor. Sistemin kırılamaması ise kullanılan gizli anahtarın elde edilememesi demektir. Kriptoanaliz ile yapılan, şifreleme sisteminde kullanılan anahtarın farklı saldırı yöntemleri ile ne kadar sürede, ne kadar kaynak harcayarak ve ne kadar veri ile elde edilebilir olduğunu bulmakla ilgilidir.

2.2 Kriptoanaliz Yaklaşım Tipleri

Kriptoanaliz yaklaşım tiplerini temel olarak iki ayrı başlık altında toplayabiliriz. Bu yaklaşımlar, saldırılan hedef açısından birbirinden ayrılmaktadır. Burada hedef olarak kastedilen, şifreleme sisteminin teorisi ve uygulamasıdır.

2.2.1 Elektronik Kriptoanaliz

Elektronik kriptoanalizde hedef, şifreleme sisteminin uygulanmasına yöneliktir. Algoritmaların uygulanması sırasında meydana gelen ayırt edici özelliklerden faydalanılmaktadır. Örneğin, anahtarda yer alan bitlerin 1 veya 0 olmasına göre şifrelemenin farklı sürelerde tamamlanması veya farklı miktarda güç çekilmesi, anahtarın tahmin edilebilmesine olanak sağlamaktadır.

Elektronik kriptoanaliz ile şifreleme sistemi, giriş ve çıkışları olan bir kutu olarak görülmeyip, sistemin içinden bir şeyleri izlenip saldırı yapılmaktadır. Zaten bu nedenle yan kanal saldırıları olarak da geçmektedir bu yaklaşım.

2.2.2 Matematiksel Kriptoanaliz

Matematiksel kriptoanalizde hedef, algoritmanın zayıflıklarından faydalanmaktadır. Örneğin, algoritmada, iki giriş farkı ile bunların çıkışları farkı arasında bir ilişki kurulabiliniyorsa bu zayıflıktan faydalanılarak anahtarı elde etmek için saldırılar yapılabilir.

Matematiksel analiz, şifreleme sistemini giriş ve çıkışları olan bir kutu (sistem) olarak görmektedir. Saldırılar da bu giriş ve çıkışlar baz alınarak yapılmaktadır.

2.2.3 İki Yaklaşımın Karşılaştırılması

Matematiksel analiz ile kırılması seneler alabilen bir şifreleme sistemi yan kanal saldırıları ile dakikalar mertebesinde kırılabilmektedir. Fakat yan kanal saldırılarının yapılabilmesi için şifreleme yapılırken kaynağın da elde olması gerekir. Elde sadece şifreleme sisteminin giriş ve çıkışları varken yan kanal saldırıları yapılamamaktadır. Bu durumda sadece matematiksel yaklaşım uygulanabilir, çünkü matematiksel yaklaşım sadece giriş ve çıkışlarla ilgileniyor.

3 MATEMATİKSEL KRİPTOANALİZ

3.1 Tanım

Matematiksel kriptoanaliz, şifreleme sisteminde algoritma baz alınarak yapılan analiz olarak tanımlanabilir. Algoritmanın özelliğine göre faklı tip saldırılar yapılarak sistemin sağlamlığı araştırılmaktadır.

3.2 Yöntemler

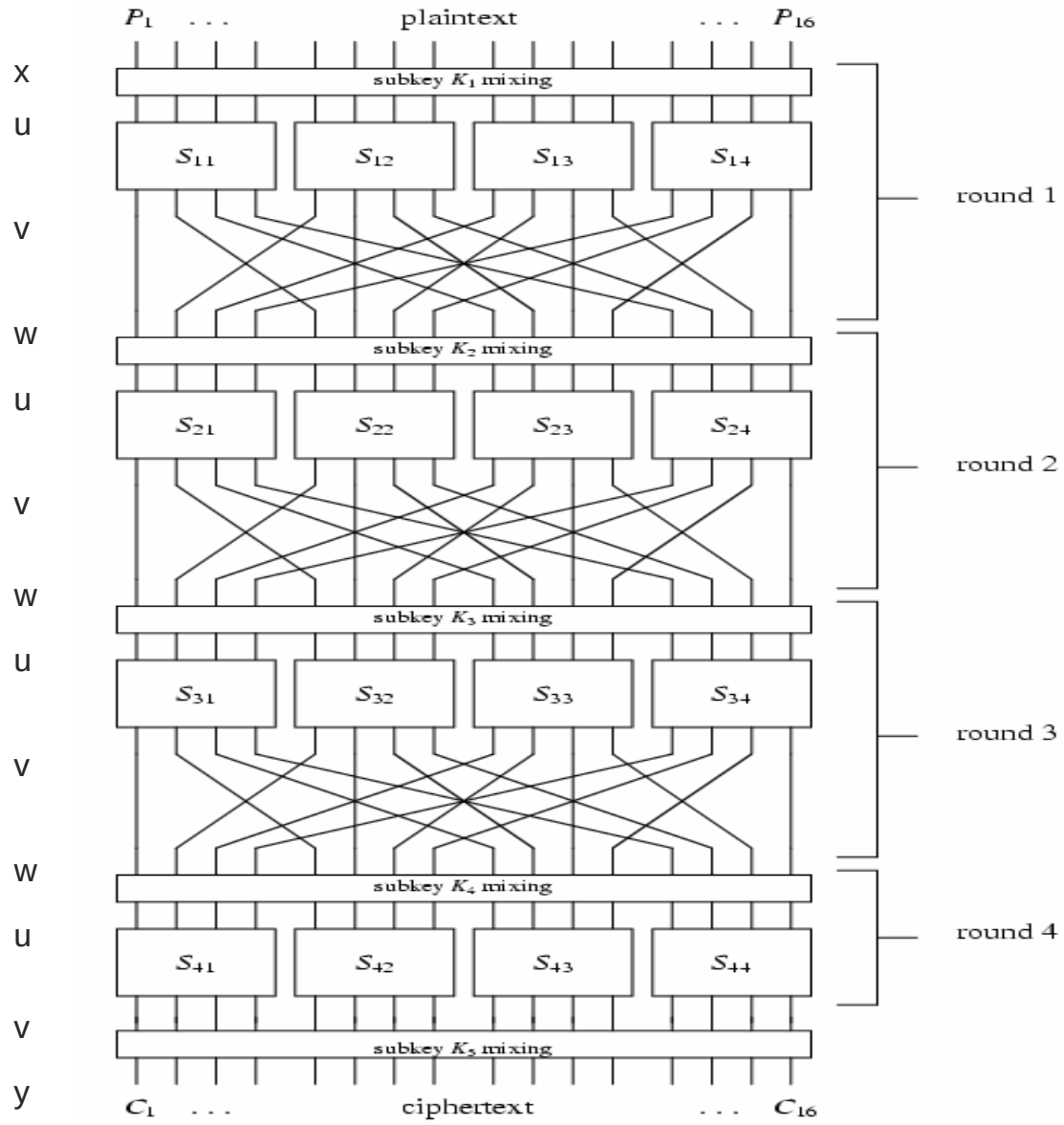
Algoritmaların yapılarına göre faklı saldırı yöntemleri bulunmaktadır. Bu yöntemlerde bazıları bazı algoritmalarda işe yararken bazıları işe yaramamaktadır. Bu tamamen kullanılan algoritmaya bağlıdır. Lineer analiz, farksal analiz, integral analiz bu yöntemlere örnek olarak verilebilir. Bunlara benzer bir çok analiz yöntemi bulunmaktadır. Lineer analizde sistem bir olasılığa bağlı olara lineerleştirilmeye çalışılır, faksal analizde iki giriş fakı ile bu girişlere bağlı çıkış farkları arasında ilişki kurulmaya çalışılır vb. Bu çalışma kapsamında lineer analiz detaylı bir şekilde anlatılmıştır.

4 SP NETWORK

Bu çalışmada lineer analiz bir SP ağı üzerinde anlatılacağı için öncelikle SP ağı hakkında bilgi verilmek istenmiştir.

SPN (Substitution-Permutation Network) bir şifreleme yapısı olup yer alma (substitution) ve yer değiştirme (permutatiton) işlemlerinin art arda belli bir sayıda uygulanmasından ibarettir. Bu belli sayı raunt sayısını ifade etmektedir. Her bir yer alma ve yer değiştirme işlemi bir raundu oluşturur.

Bir SPN yapısı şekil 1 de görülmektedir.



Şekil 1

Her rauntta yer alma ve yer değiştirme işlemleri yanı sıra bir de her raunt için oluşturulan anahtar kullanılır. Bu anahtarlar şifreleme sisteminin ana anahtarı kullanılarak açık olarak bilinen bir algoritma tarafından üretilir.

Şifreleme, şekil 2 de görülüğü gibi yapılmaktadır.

$$
\begin{aligned}
w^0 &\leftarrow x \\
w^1 &\leftarrow g(w^0, K^1) \\
w^2 &\leftarrow g(w^1, K^2) \\
&\vdots \\
w^{Nr-1} &\leftarrow g(w^{Nr-2}, K^{Nr-1}) \\
w^{Nr} &\leftarrow g(w^{Nr-1}, K^{Nr}) \\
y &\leftarrow w^{Nr}
\end{aligned}
$$

Şekil 2

Şekil 2 de her bir rauntta yapılan işlem g fonksiyonu ile ifade edilmiştir. Yani g fonksiyonu raunt anahtarı ile yapılan işlemi, yer alma (substitution) işlemini ve yer değiştirme (permutation) işlemini içermektedir.

Şifre çözme ise şekil 3 de görüldüğü gibi yapılmaktadır.

$$
\begin{aligned}
w^{Nr} &\leftarrow y \\
w^{Nr-1} &\leftarrow g^{-1}(w^{Nr}, K^{Nr}) \\
&\vdots \\
w^1 &\leftarrow g^{-1}(w^2, K^2) \\
w^0 &\leftarrow g^{-1}(w^1, K^1) \\
x &\leftarrow w^0
\end{aligned}
$$

Şekil 3

Şekil 3 de görüldüğü gibi şifre çözülebilmesi için g fonksiyonunun birebir ve örten olması gerekir ki tersi bulunabilsin.

SPN şifreleme sisteminin matematiksel olarak ifadesini aşağıdaki şekilde yazabiliriz; SPN şifreleme sistemi

$$(x, \pi_S, \pi_P, (K^1, ..., K^{Nr+1}))$$

dörtlüsünden oluşur, burada

x şifrelenecek bilgiler kümesi

$\pi_S : \{0,1\}^l \rightarrow \{0,1\}^l$ $\qquad P = C = \{0,1\}^{lm}$

$\pi_P : \{1,...,lm\} \rightarrow \{1,...,lm\}$ $\qquad K \subseteq (\{0,1\}^{lm})^{Nr+1}$

Şifreleme algoritması şekil 4 de yer almaktadır.

$$
\begin{aligned}
& w^0 \leftarrow x \\
& \text{for } r \leftarrow 1 \text{ to } Nr-1 \\
& \quad \text{do} \begin{cases} u^r \leftarrow w^{r-1} \oplus K^r \\ \text{for } i \leftarrow 1 \text{ to } m \\ \quad \text{do } v^r_{(i)} \leftarrow \pi_S(u^r_{(i)}) \\ w^r \leftarrow (v^r_{\pi_P(1)}, \ldots, v^r_{\pi_P(lm)}) \end{cases} \\
& u^{Nr} \leftarrow w^{Nr-1} \oplus K^{Nr} \\
& \text{for } i \leftarrow 1 \text{ to } m \\
& \quad \text{do } v^{Nr}_{(i)} \leftarrow \pi_S(u^{Nr}_{(i)}) \\
& y \leftarrow v^{Nr} \oplus K^{Nr+1} \\
& \text{output } (y)
\end{aligned}
$$

Şekil 4

5 LİNEER KRİPTOANALİZ

Lineer analiz yapabilmek için elde metin ve şifreli metin çiftleri olması gerekir. Elde bu bilgiler varken analizin nasıl yapılacağı aşağıda anlatılmıştır.

Lineer kriptoanalizde yapılan işlem, sistemin lineer bir modelinin çıkartılması ve bu model kullanılarak son rauntta anahtarın tahmin edilmesine dayanır. İncelenilen SP ağında yapılan işlemler raunt anahtarları ile “dar veya” işlemi, yer alma (substitution) ve yer değiştirme (permutation) işlemleriydi. “dar veya” ve “yer değiştirme işlemleri” zaten lineer olduğu için geriye yalnızca “s-box” dediğimiz yer alma (substitution) işlemlerini yapan kısmın lineerleştirilmesi kalıyor.

Burada lineerleştirmeden kastedilen giriş bitleri ile çıkış bitleri arasında “dar veya” işlemine dayanan bir ilişki kurulması.

s-box lar karakterleri itibari ile lineer olmadıkları için bunların lineerleştirme işlemleri bir olasılıkla yapılmaktadır. Bunun için öncelikle öncül bir teoremden bahsetmek gerekiyor.

X1, X2,… {0,1} değerlerini alan rastlantı değişkenleri olsun, ve bunların olasılık değerleri ;

$$\Pr[X_i = 0] = p_i\,, \qquad i = 1,2,...$$
$$\Pr[X_i = 1] = 1 - p_i\,, \quad i = 1,2,...$$

Xi, Xj bağımsız ise aşağıdaki eşitlikleri sağlandığı görülebilir;

$$\Pr[X_i = 0, X_j = 0] = p_i p_j$$
$$\Pr[X_i = 0, X_j = 1] = p_i(1 - p_j)$$
$$\Pr[X_i = 1, X_j = 0] = (1 - p_i)p_j$$
$$\Pr[X_i = 1, X_j = 1] = (1 - p_i)(1 - p_j)$$

Burada "bias" tanımını yapacak olursak ;

$$\varepsilon_i = p_i - \tfrac{1}{2}$$

"Bias" ne kadar yüksek olasılıkla sistemi lineerleştirmeyi başardığımız konusunda fikir verecek, bu nedenle bu tanıma şu an ihtiyaç duyulmuştur.

"Bias"in aşağıdaki aralıkta olduğu ve raslantı değişkenlerinin değerlerinin "bias" cinsinden eşiti aşağıda görülmektedir.

$$-\tfrac{1}{2} \le \varepsilon_i \le \tfrac{1}{2}\,,$$
$$\Pr[X_i = 0] = \tfrac{1}{2} + \varepsilon_i\,,$$
$$\Pr[X_i = 1] = \tfrac{1}{2} - \varepsilon_i\,.$$

İşlemlerimizde "dar veya" işlemini kullanacağımız için bu işlemin olasılık üzerinde etkisini inceleyecek olursak;

$$X_i \oplus X_j$$

$$\Pr[X_i \oplus X_j = 0] = p_i p_j + (1 - p_i)(1 - p_j)$$
$$\Pr[X_i \oplus X_j = 1] = p_i(1 - p_j) + (1 - p_i)p_j$$

Sonucuna varabiliriz. "Bias" açısından bakacak olursak $X_{i_1} \oplus \cdots \oplus X_{i_k}$ rastlantı değişkeninin bias değeri $\varepsilon_{i_1, i_2, \ldots, i_k}$; olsun.

Gösterilmesi tümevarım ile sağlanabilen aşağıdaki ifade yazılabilir;

$$\varepsilon_{i_1,i_2,\ldots,i_k} = 2^{k-1} \prod_{j=1}^{k} \varepsilon_{i_j} \quad .$$

Sistemin lineerleştirilmesi için önce s-box ların lineerleştirilmesi yapılıp sonra tüm sisteminki yapılacağı için bias hesabında yukarıdaki ifade kullanılacaktır.

5.1 S-box'ların Lineerleştirilmesi

s-box, giriş ve çıkışları aşağıdaki gibi olan bir kutu şeklinde düşünülebilir.

$$\pi_S : \{0,1\}^m \rightarrow \{0,1\}^n$$

Giriş ve çıkışların olasılıkları ile ilgili şu eşitlikler yazılabilir;

$$(y_1,\ldots,y_n) \neq \pi_S(x_1,\ldots,x_m) \Rightarrow$$
$$\Pr[X_1 = x_1,\ldots,X_m = x_m, Y_1 = y_1,\ldots,Y_n = y_n] = 0$$
$$(y_1,\ldots,y_n) = \pi_S(x_1,\ldots,x_m) \Rightarrow$$
$$\Pr[X_1 = x_1,\ldots,X_m = x_m, Y_1 = y_1,\ldots,Y_n = y_n] = 2^{-m}$$

Burada ikinci olasılık değerinin 2^(-m) olmasının nedeni y değerlerinin x değerlerine bağlı olması.

Girişin bazı bitleri ile çıkışın bazı bileri arasında ilişki kurmanın olasılığının hesaplanması için şekil 5 de yer alan tablo kullanılabilir;

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$	$X_1 \oplus X_4$	Y_2	$X_3 \oplus X_4$	$Y_1 \oplus Y_4$
0	0	0	0	1	1	1	0	0	0	0	1	0	1
0	0	0	1	0	1	0	0	0	0	1	1	1	0
0	0	1	0	1	1	0	1	1	0	0	1	1	0
0	0	1	1	0	0	0	1	1	1	1	0	0	1
0	1	0	0	0	0	1	0	1	1	0	0	0	0
0	1	0	1	1	1	1	1	1	1	1	1	1	0
0	1	1	0	1	0	1	1	0	1	0	0	1	0
0	1	1	1	1	0	0	0	0	1	1	0	0	1
1	0	0	0	0	0	1	1	0	0	1	0	0	1
1	0	0	1	1	0	1	0	0	0	0	0	1	1
1	0	1	0	0	1	1	0	1	1	1	1	1	0
1	0	1	1	1	1	0	0	1	1	0	1	0	1
1	1	0	0	0	1	0	1	1	1	1	1	0	1
1	1	0	1	1	0	0	1	1	0	0	0	1	0
1	1	1	0	0	0	0	0	0	0	1	0	1	0
1	1	1	1	0	1	1	1	0	0	0	1	0	1

Şekil 5

Mesela buradan $X_1 \oplus X_4 \oplus Y_2 = 0$ olasılığını bulmak için bu ifadenin sağlandığı satır sayısını 16 ya (toplam satır sayısı) böleriz. Böylece bu s-box için bir lineerleştirme yapmış oluruz, yani giriş ile çıkış arasında bir lineer ifade bulmuş oluruz ve ne kadarlık bir olasılıkla doğru olduğunu da hesaplamış oluruz.

Bias değerini de zaten $\varepsilon_i = p_i - \frac{1}{2}$ formülüyle bulabiliyoruz.

$X_1 \oplus X_4 \oplus Y_2 = 0$ gibi toplam 2^8 = 256 farklı lineerleştirme yapılabilir ve her bir lineerleştirmenin kaç tanesinin gerçekten doğru sonuç verdiği hesaplanabilir. Bunları bir tablo ile gösterecek olursak; şekil 6 daki gibi bir tablo oraya çıkacaktır;

		Output Sum															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Input Sum	0	+8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	−2	−2	0	0	−2	+6	+2	+2	0	0	+2	+2	0	0
	2	0	0	−2	−2	0	0	−2	−2	0	0	+2	+2	0	0	−6	+2
	3	0	0	0	0	0	0	0	0	+2	−6	−2	−2	+2	+2	−2	−2
	4	0	+2	0	−2	−2	−4	−2	0	0	−2	0	+2	+2	−4	+2	0
	5	0	−2	−2	0	−2	0	+4	+2	−2	0	−4	+2	0	−2	−2	0
	6	0	+2	−2	+4	+2	0	0	+2	0	−2	+2	+4	−2	0	0	−2
	7	0	−2	0	+2	+2	−4	+2	0	−2	0	+2	0	+4	+2	0	+2
	8	0	0	0	0	0	0	0	0	−2	+2	+2	−2	+2	−2	−2	−6
	9	0	0	−2	−2	0	0	−2	−2	−4	0	−2	+2	0	+4	+2	−2
	A	0	+4	−2	+2	−4	0	+2	−2	+2	+2	0	0	+2	+2	0	0
	B	0	+4	0	−4	+4	0	+4	0	0	0	0	0	0	0	0	0
	C	0	−2	+4	−2	−2	0	+2	0	+2	0	+2	+4	0	+2	0	−2
	D	0	+2	+2	0	−2	+4	0	+2	−4	−2	+2	0	+2	0	0	+2
	E	0	+2	+2	0	−2	−4	0	+2	−2	0	0	−2	−4	+2	−2	0
	F	0	−2	−4	−2	−2	0	+2	0	0	−2	+4	−2	−2	0	+2	0

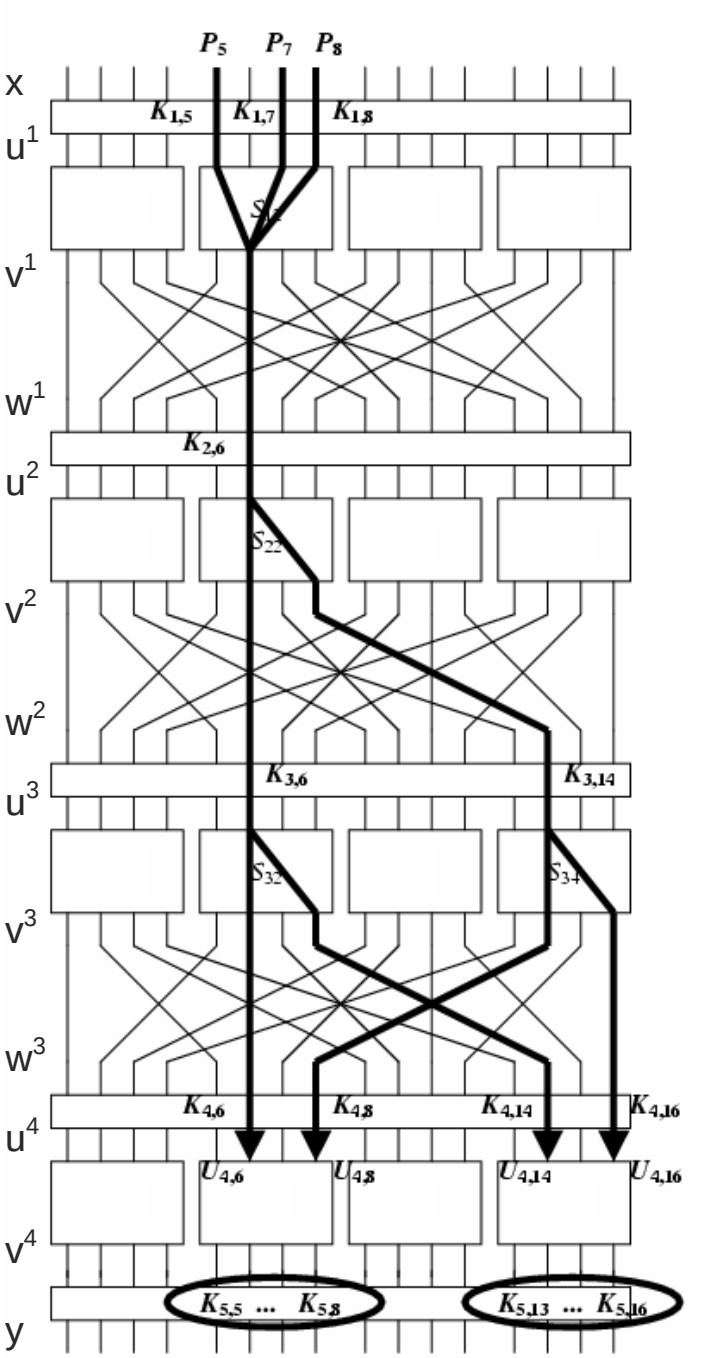
Şekil 6

Her bir hücredeki değer, sağlanan satır sayısı – 8 değerini içerir. Bu değeri de 16 ya böldüğümüzde her bir lineer ifade için bias değeri hesaplanmış oluruz.

5.2 SP Ağının Lineerleştirilmesi

s-box ların lineerleştirilmesinden sonra asıl hedef olan sistemin tamamının lineerleştirilmesi kısmı kalıyor yapılacak saldırı için.

Şimdi sırada ağ içinde hangi s-box'ların ve bunların hangi giriş ve çıkış bitlerinin seçileceği kararı bulunuyor. Burada yapılacak olan şekil 7 deki gibi fazla budaklanmaya neden olmayacak ve sıfırdan en uzak bias değerini verecek şekilde bu seçimin yapılmasıdır.



Şekil 7

Şekil 7 de birinci rauntta ikinci s-box'ın seçildiği ve bu s-box'ın da gösterilen 3 giriş biti ile çıkıştaki tek biti arasında lineer ilişki kurulduğu görülmektedir. Yani lineer ilişkiyi yazacak olursak ;
X1 + X3 + X4 = Y2 (burada '+' lar dar veya işlemini ifade ediyor)
Ve bunun sağlandığı bias değerini bulmak istersek ¼ olduğunu görürüz.

Benzer şekilde aşağıdaki şekilde bias değerleri yazılabilir kullanılan 4 s-box için;

$T_1 = U_5^1 \oplus U_7^1 \oplus U_8^1 \oplus V_6^1$ Bias : 1/4

$T_2 = U_6^2 \oplus V_6^2 \oplus V_8^2$ Bias : -1/4

$T_3 = U_6^3 \oplus V_6^3 \oplus V_8^3$ Bias : -1/4

$T_4 = U_{14}^3 \oplus V_{14}^3 \oplus V_{16}^3$ Bias : -1/4

Bu dört ifadeyi de birleştirirsek; $T_1 \oplus T_2 \oplus T_3 \oplus T_4$ "bias" değerinin öncül teoremden 23(1/4)(-1/4)3=-1/32 olduğunu görebiliriz.

Burada bulunan "bias" değeri, gerekli olan metin – şifreli metin çiftinin sayısının belirlenmesinde önemli olmaktadır.

Yaklaşık olarak gerekli olan veri çifti sayısı Cx"bias"^(-2) şekinde ifade edilmektedir. Burda C küçük bir sayıdır.

Şimdi yapılacak olan $T_1 \oplus T_2 \oplus T_3 \oplus T_4$ ten faydalanarak sisteme giriş ile (X) son raunttan bir önceki raunttun çıkışları arasındaki lineer ilişkiyi göstermek oluyor.

Ahahtar ile dar veya işleminin çıkışı olan U lar yerine eşitini yazınca aşağıdaki ifadeler oluşuyor,

$$
\begin{aligned}
T_1 &= U_5^1 \oplus U_7^1 \oplus U_8^1 \oplus V_6^1 = X_5 \oplus K_5^1 \oplus X_7 \oplus K_7^1 \oplus X_8 \oplus K_8^1 \oplus V_6^1 \\
T_2 &= U_6^2 \oplus V_6^2 \oplus V_8^2 \qquad = V_6^1 \oplus K_6^2 \oplus V_6^2 \oplus V_8^2 \\
T_3 &= U_6^3 \oplus V_6^3 \oplus V_8^3 \qquad = V_6^2 \oplus K_6^3 \oplus V_6^3 \oplus V_8^3 \\
T_4 &= U_{14}^3 \oplus V_{14}^3 \oplus V_{16}^3 \qquad = V_8^2 \oplus K_{14}^3 \oplus V_{14}^3 \oplus V_{16}^3
\end{aligned}
$$

Bu dört ifadenin "dar veya" sı (3.1) deki ifadeyi veriyor

$$
\begin{aligned}
X_5 \oplus X_7 \oplus X_8 \oplus V_6^3 \oplus V_8^3 \oplus V_{14}^3 \oplus V_{16}^3 \\
\oplus K_5^1 \oplus K_7^1 \oplus K_8^1 \oplus K_6^2 \oplus K_6^3 \oplus K_{14}^3 \qquad (3.1)
\end{aligned}
$$

(3.1) deki ifade ile aşağıdaki eşitlikler birleştirilince de (3.2) deki ifade elde ediliyor. Aşağıdaki eşitlikler network yapısına şekilden bakınca rahatlıkla görülebilir;

$$V_6^3 = U_6^4 \oplus K_6^4 \qquad V_8^3 = U_{14}^4 \oplus K_{14}^4$$
$$V_{14}^3 = U_8^4 \oplus K_8^4 \qquad V_{16}^3 = U_{16}^4 \oplus K_{16}^4$$

$$X_5 \oplus X_7 \oplus X_8 \oplus U_6^4 \oplus U_8^4 \oplus U_{14}^4 \oplus U_{16}^4$$
$$\oplus K_5^1 \oplus K_7^1 \oplus K_8^1 \oplus K_6^2 \oplus K_6^3 \oplus K_{14}^3 \oplus K_6^4 \oplus K_8^4 \oplus K_{14}^4 \oplus K_{16}^4 \quad (3.2)$$

(3.2), sadece metin bitleri, son raunttan bir önceki raunttun çıkış bitleri ve anahtar bitlerinden oluşuyor. Anahtar bitleri sabit olduğu için

$$K_5^1 \oplus K_7^1 \oplus K_8^1 \oplus K_6^2 \oplus K_6^3 \oplus K_{14}^3 \oplus K_6^4 \oplus K_8^4 \oplus K_{14}^4 \oplus K_{16}^4$$

ifadesi 0 ya da 1 değerini alabilir. Bu, lineerleştirme etkisi üzerinde bir öneme sahip olmadığı için ihmal edilebilir ve son durumda ifade (3.3) deki şekle gelir;

$$X_5 \oplus X_7 \oplus X_8 \oplus U_6^4 \oplus U_8^4 \oplus U_{14}^4 \oplus U_{16}^4 \qquad (3.3)$$

Artık giriş ile son raunttan bir önceki raunt arasında lineer bir denklem sağlanmış oluyoruz ve bias değeri -1/32 veya 1/32 yukarıda ihmal ettiğimiz ifadenin 0 yada 1 olmasına bağlı olarak.

Bu lineerleştirmede ifadedeki çıkış bitleri son rauntta hangi s-boxların giriş bitleri ise o s-boxlara bağlı olan çıkışlardaki bitlere denk düşen anahtar bitlerini tahmin edebilir duruma geliyoruz. Sonda kullanılan anahtarın diğer bitlerini de tahmin etmek için başka s-box lar aktif olarak kullanılmalı.

Yapılan lineerleştirmeden etkilenen anahtar bitleri sayısı şekil 7 dan da görüleceği üzere 8 bit, ve elimizde toplam T adet veri çifti (metin – şifreli metin) mevcut. Bitlerin her bir dağılımı için bu T adet verinin kaç tanesi sağlandığı hesaplanır, ve bunlardan sağlayan sayısı (T/2-T/32 , T/2 + T/32) aralığında olan doğru bitlerdir denilir.

Burada etkilenen anahtar bitleri sayısı ne kadar fazla olursa o kadar fazla denenme yapılacak demek oluyor, bu nedenle s-box ları seçerken fazla dallanma olması istenmiyor. Bunun yerine bir s-box grubu daha seçilir ve anahtarın diğer 8 biti bulunur. Böylece 2 x 2^8 x T x k sürede anahtar bulunabilir, 2^16 x T x k yerine. Süre 128 de 1 ine iniyor.

Lineer kriptoanaliz algoritması şekil 8 de yer almaktadır.

$$
\begin{array}{l}
\text{for } (L_1, L_2) \leftarrow (0,0) \text{ to } (F, F) \\
\quad \text{do } Count[L_1, L_2] \leftarrow 0 \\
\text{for each } (x, y) \in \tau \\
\text{do}\begin{cases}
\text{for } (L_1, L_2) \leftarrow (0,0) \text{ to } (F, F) \\
\text{do}\begin{cases}
v^4_{(2)} \leftarrow L_1 \oplus y_{(2)} \\
v^4_{(4)} \leftarrow L_2 \oplus y_{(4)} \\
u^4_{(2)} \leftarrow \pi_S^{-1}(v^4_{(2)}) \\
u^4_{(4)} \leftarrow \pi_S^{-1}(v^4_{(4)}) \\
z \leftarrow x_5 \oplus x_7 \oplus x_8 \oplus u^4_6 \oplus u^4_8 \oplus u^4_{14} \oplus u^4_{16} \\
\text{if } z = 0 \\
\quad \text{then } Count[L_1, L_2] \leftarrow Count[L_1, L_2] + 1
\end{cases}
\end{cases} \\
max \leftarrow -1 \\
\text{for } (L_1, L_2) \leftarrow (0,0) \text{ to } (F, F) \\
\quad \text{do}\begin{cases}
Count[L_1, L_2] \leftarrow |Count[L_1, L_2] - T/2| \\
\text{if } Count[L_1, L_2] > \max \\
\quad \text{then}\begin{cases}
max \leftarrow Count[L_1, L_2] \\
maxkey \leftarrow (L_1, L_2)
\end{cases}
\end{cases} \\
\text{output } (maxkey)
\end{array}
$$

Şekil 8

6 SONUÇ

Matematiksel kriptoanalizlerden bir tanesi olan lineer analiz belli bir olasılıkla sistemin lineerleştirilmesine dayanıyor. Bu, lineerleştirilmiş model kullanılarak sonda kullanılan anahtar bulunuyor. Lineerleştirme için ise sistem için de lineer olmayan s-box ların lineerleştirilmesi gerekiyor. Hangi lineer model ne kadar olasılıkla doğru bunlar hesaplanıyor ve bunlardan olasılığı yüksek olanlar seçilmeye çalışılıyor. Sistemin lineer modeli çıkartılırken de belli kurallara uyuluyor, hangi s-box lar aktif olarak seçilecek bunların hangi bitleri dikkate alınacak kararını vermek için.

7 KAYNAKLAR

[1] Douglas R. Stinson, “Cryptography Theory and Practice”, Boca Raton, FL : Chapman & Hall/CRC, 2002.

[2] http://www.wikipedia.org